REMARKS

Reconsideration of this application, as presently amended, is respectfully requested.

Claims 1-23 are pending in this application. Claims 1-23 stand rejected.

Claim Objections

Claims 9 and 15 were objected to for informalities.

Specifically, claim 9 was objected for reciting the limitation "a individual" in line 2. Claim 9 has been amended to change "a individual" to --an individual--. Further, it is noted that claim 8 has been amended similarly.

Claim 15 was objected to for reciting "personalisation" in line 2. Claim 15 has been amended to change "personalisation" to --personalization--. It is noted that claims 8 and 18 have also been amended to change "authorised" to --authorized--.

Finally, the claims have been amended to improve form in accordance with preferred U.S. practice.

In view of the above amendments, withdrawal of the objections to the claims is respectfully requested.

Claim Rejection – 35 U.S.C. §112, second paragraph

Claims 1, 9 and 16 were rejected under 35 U.S.C. §112, second paragraph, for alleged indefiniteness.

More specifically, with respect to claim 1, the Examiner alleges (1) there is insufficient antecedent basis for the recitation "the provider of the protected area" in claim 1, line 10; and (2) the recitation "authentication and/or communication exclusively of the unique identifier of the second network to the provider of the protected area by means of the authentication unit" is confusing and not clearly defined.

Claim 1 has been amended to obviate the rejection based on lack of antecedent basis.

Further, claim 1, lines 13-15, has been amended to recite "authenticating the unique connection identifier of the second network and/or communicating the unique connection identifier of the second network to the provider of the protected area by means of the authentication unit." It is believed that this amendment to claim 1 clearly defines the invention, in a manner consistent with, e.g., page 8, line 22 – page 9, line 2 of the application specification, which describes the customer's IP address being used to authenticate the unique connection identifier. The unique connection identifier may then be communicated from the authentication unit 16 to the internal network database server 10.

With respect to claim 9, the Examiner asserts that the recitation "before release of a individual connection identification, a further entry on the terminal is necessary in addition" is not clearly defined. Claim 9 has been amended to improve form and grammar, and now recites "before release of an individual connection identification, a further entry on the terminal is necessary."

However, it is believed that both the current language of claim 9 and the original language of claim 9 clearly define the invention. In particular, it is believed that the language of

claim 9 clearly defines the aspect of the invention described, e.g., on page 9, lines 1-5 of the application specification.

With respect to claim 16, the Office Action asserts (1) there is insufficient antecedent basis for the claim 16 recitations "the different identifiers", "the other unique identifiers" and "the data" in lines 6 and 8-9; and (2) the recitation "authentication and/or issue exclusively of one of the unique identifiers when a corresponding enquiry is made regarding the other unique identifiers" is not clearly defined.

Claim 16 has been amended to obviate the rejection based on lack of antecedent basis.

Further, claim 16 has been amended to recite "authenticating and/or issuing of one of the unique identifiers when a corresponding enquiry is made regarding an other of the unique identifiers." It is believed that this amendment to claim 16 clearly defines the invention in a manner consistent with the description, e.g., on page 8, line 22 – page 9, line 2 of the application specification.

In view of the above amendments and remarks, reconsideration and withdrawal of the rejection under §112, second paragraph, are respectfully requested.

Rejection in view of the Prior Art

Claims 1-23 were rejected under 35 U.S.C. §102(e) as being anticipated by **Nakajima** (US 2003/0169714). For the reasons set forth in detail below, this rejection is respectfully traversed.

Independent claim 1 recites a method for automatically identifying an access right to protected areas in a first network using a unique connection identifier of a second network, comprising the following procedural steps: dynamic or static assignment of a unique identifier of the first network for a terminal, during or prior to the latter's **connection to the first network by means of the second network** (emphasis added); storage of a combination of at least the unique connection identifier of the **second network by means of which the connection was made** (emphasis added), and the unique identifier of the first network in an authentication unit; **a provider of the protected area requesting** (emphasis added) the authentication unit to determine the unique connection identifier of the second network using the unique identifier of the first network when the terminal would like access to the protected area; authenticating (only) **the unique connection identifier of the second network** (emphasis added) and/or communicating (only) **the unique connection identifier of the second network** (emphasis added) to the provider of the protected area by means of the authentication unit; and checking whether an access right for the protected area exists for the unique connection identifier of the second network.

Nakajima discloses a method and an apparatus for providing communication services.

With respect to the method described in **Nakajima** for providing communication service, a service terminal 101 has a static IP address assigned thereto as well as a further ID. The service terminal 101 is connected via a line (first network) with a service gateway 102. The service gateway 102 manages IP addresses in order to control access to the internet 104 (second network).

In order to access the internet, the service terminal 101 initiates a connection to a mobile phone 105, in order to transmit its IP address to the mobile phone 105. The mobile phone 105 then initiates a connection via a communication network 100 (third network) to a subscriber system 103 and transmits the IP address of the terminal 101 as well as the phone number of the mobile phone 105 to the subscriber system 103. After the data are transmitted, the connection between the mobile phone 105 and the subscriber system 103 is terminated.

The subscriber system 103 then performs a user authentication process with respect to mobile terminal 105, and if authentication is successful, forwards the associated IP address to the service gateway 102. The service gateway 102 then provides the connection between the internet 104 and the service terminal 101 having the above IP address assigned thereto. At this point it is ensured that billing for the use of the Internet service may be done via the number of the mobile phone.

The method recited in claim 1 thus differs from the method taught by the **Nakajima** reference in the following points:

- According to claim 1, connection to the first network is achieved **via the second network**. In contrast, in **Nakajima**, the connection to the first network is achieved via the line between the service terminal and the service gateway but not via the communication network 100 of the mobile phone. This connection is only used for a single transmission of data between the mobile phone and the subscriber system.

- According to claim 1, a combination of the unique connection identifier of the second network, **via which the connection is established**, and the unique identifier of the first

network **are stored in an authentication unit**. Unlike the claimed invention, such storage of a combination of data is not described in a authentication unit according to **Nakajima**, and indeed does not appear to be necessary. In **Nakajima**, only a single authentication followed by a clearance is described, i.e., once the authentication is successful, the subscriber system indicates to the service gateway that the connection to the internet may be provided and thereafter the data is no longer required.

- According to claim 1, the provider of the protected area **requests** the authentication unit to determine the unique connection identifier of the second network using the unique identifier of the first network, when the terminal would like access to the protected area. In contrast, in **Nakajima** such a request is not present. The subscriber unit 103 automatically issues a single clearance for a specific IP address to the service gateway 102. This is also the reason why storage of the above referenced data combination is not necessary in an authentication unit.

- According to claim 1, **authenticating the unique connection identifier** of the second network and/or communicating the unique connection identifier of the second network to the provider of the protected area by means of the authentication unit is performed. Unlike the claimed invention, such an authentication is not disclosed in **Nakajima** due to the fact that the corresponding request by the provider is not present.

- Finally, according to claim 1, it is checked whether an access right for the protected area exists for the unique connection identifier of the second network. In contrast, such a checking of access rights is also not disclosed in **Nakajima**.

The present invention intends to increase security while accessing protected areas in networks, which is achieved by the above referenced steps. It is particularly relevant that for authentication of access rights, **a combination of unique network identifiers of two networks is used** and that the **connection to one of the networks** (the one having the protected area which is to be accessed) **occurs via the other network.** In so doing, increased security may be achieved, as discussed in some detail throughout the application specification.

In the method according to **Nakajima**, a connection via the service terminal and the service gateway (first network) as well as between the service gateway and the internet (second network) is provided. Identification data are transmitted via a separate network (communication network 100) to the service gateway. Thus, a combination of network identifiers according to claim 1 is clearly not provided.

Furthermore, according to **Nakajima** the required identification data consisting of IP address and telephone number are not stored, as recited in claim 1 of the present application, in order to allow one or several requests by a provider of a protected area to determine proper authentication.

According to **Nakajima** a single clearance is automatically provided to the service gateway 101 via the subscriber system 103. Providers of protected areas in the internet do not have the possibility to authenticate access rights to their protected areas, inasmuch as no data storage is provided for in the subscriber system 103, and it is not possible to post such a request to the subscriber system 103 according to **Nakajima**.

Regarding independent claim 16, the same arguments provided above with respect to claim 1 similarly apply to independent method claim 16, which additionally comprises automatic deletion of data from the authentication unit, if a connection to at least one of the two networks is terminated. This feature additionally increases security, inasmuch as upon termination, the authentication data are automatically deleted and may thus not be misused.

This feature is clearly also not shown or disclosed in **Nakajima**, inasmuch as the communication via the mobile phone is only for providing once the IP address and the phone number to the subscriber system and thereafter the connection between the mobile phone and the subscriber system is terminated.

In view of the above amendments and remarks, it is respectfully submitted that independent claims 1 and 16, and claims 2-15 and 17-23 depending therefrom, patentably distinguish over the cited prior art and therefore define allowable subject matter. Reconsideration and withdrawal of the rejection under §102 are respectfully requested.

CONCLUSION

In view of the foregoing amendments and accompanying remarks, it is submitted that all pending claims are in condition for allowance. A prompt and favorable reconsideration of the rejection and an indication of allowability of all pending claims are earnestly solicited.

If the Examiner believes that there are issues remaining to be resolved in this application, the Examiner is invited to contact the undersigned attorney at the telephone number indicated below to arrange for an interview to expedite and complete prosecution of this case.
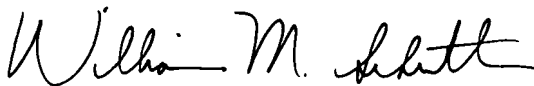
If this paper is not timely filed, Applicants respectfully petition for an appropriate extension of time. The fees for such an extension or any other fees that may be due with respect to this paper may be charged to Deposit Account No. 50-2866.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP

William M. Schertler
Attorney for Applicants
Registration No. 35,348
Telephone: (202) 822-1100
Facsimile: (202) 822-1111

WMS/dlt